



Colorado Springs Police Department Standard Operating Procedure

DL-1501-12 Automated License Plate Reader System (ALPRS)

Section 1500 – Assigned Equipment

Effective Date: 3/24/2026

Supersedes Date: 2/5/2026

.01 Purpose

The purpose of this directive is to specify procedures for the use of Automated License Plate Reader Systems (ALPRS) and the use, maintenance, and storage of digital data collected by this technology.

.02 Cross Reference

[GO 400 Employee Conduct](#)

[GO 305 Immigration and Foreign Nationals](#)

[DL-600-01 Allegations of Employee Misconduct](#)

.03 Definitions

Alert (also referred to as a "Hit"): A visual and/or audible real-time alert indicating a potential match between a license plate scanned by the ALPR system and a record from the hotlist.

ALPRS Administrator: An individual designated by the Metro Division Commander to manage ALPRS training and access, ensuring its appropriate use and compliance with relevant procedures.

ALPR-Generated Data: All data captured by the ALPR system, including the location, date, and time of a scanned license plate, as well as any digital photographic images of the license plate and vehicle generated by the LPR equipment.

Automated License Plate Reader System (ALPRS): A system with LPR cameras, computers, and software designed to automatically capture and interpret the characters on vehicle license plates. The collected data may be cross-referenced with a list of license plates relevant to law enforcement, such as those associated with investigations or enforcement actions. ALPR

technology on public roadways can capture vehicle license plates and other identifying characteristics that may or may not be unique to the vehicle.

Fixed ALPRS: ALPR cameras that are affixed to a structure, such as a pole. The system used by the department is an Axon system.

Hotlist: A database of license plates associated with vehicles that are linked to a specific law enforcement purpose, including active investigations, stolen vehicles or plates, wanted persons, or other articulable public safety concerns. Hotlist entries may originate from CCIC/NCIC or be manually entered by authorized personnel in accordance with this directive.

Mobile ALPRS: ALPR cameras that are affixed to an authorized vehicle for mobile deployment. The department uses two systems of mobile ALPRS: Axon and Leonardo ELSAG.

.04 Procedure

Automatic License Plate Reader Systems (ALPRS) are designed to assist and enhance law enforcement's ability to identify vehicles associated with criminal activity, recover stolen property, apprehend fugitives, support investigations, and respond to public safety incidents (e.g., missing child, suicidal person). The Colorado Springs Police Department (CSPD) has both mobile and fixed ALPRS.

ALPRS use specialized cameras and software to capture, interpret, and record license plate and vehicle information. These systems automatically compare captured data against established lists of vehicles of interest.

ALPRS captures and stores vehicle data in a searchable database, including:

- License plates and partial license plates
- Vehicle characteristics such as decals, top racks, back racks, and toolboxes attached to the vehicle
- Date, time, location, and direction of travel at the time the license plate was captured.
- Digital photographic images of the license plate and vehicle

There are two primary purposes for use of ALPRS:

- Real-time alerts
- Searches of stored data

Authorized Use

Designated personnel who have completed required training may utilize ALPRS only for official law enforcement and public safety purposes that are tied to a specific and articulable need, such

as a call for service, active investigation, or other documented public safety or law enforcement purpose. ALPR-collected data will not be used for any other purposes.

Use of ALPRS and accessing ALPRS data is subject to periodic and administrative audits to ensure compliance with this directive. Misuse of ALPRS or ALPR databases will be investigated in accordance with [DL-600-01 Allegations of Employee Misconduct](#) and may additionally result in suspension or revocation of system access.

Verification Required

An alert (hit) does not constitute confirmation that the license plate or vehicle is of interest; further investigation is required to verify the alert.

Prior to contacting vehicle occupants or taking an enforcement action based on an ALPR alert (hit), officers will take the following actions:

- Visually verify that the vehicle plate number matches the plate number and state returned by the ALPRS, including characters on the license plate and the state of issuance.
- Verify the information through the CCIC/NCIC database or other original source.

In response to a custom hotlist alert, officers must have independent reasonable suspicion or probable cause to take police action against the individual beyond the alert.

Search and Use of Stored Data

Searches and use of ALPRS data is only allowed for the authorized purposes under this directive, regardless of how the data is collected.

All personnel that search ALPRS data must indicate the case number and reason for the search in the system. The reason must be described in sufficient detail to confirm its use is for an authorized purpose related to the listed case.

Examples:

- Suspect vehicle in a DV case
- Witness vehicle in a Homicide Investigation
- Suspect vehicle in a Hit & Run
- Vehicle of Interest in a Robbery Investigation

When using searches in an investigation, additional research must be done to confirm the vehicle located on the ALPR hit is the vehicle involved in the current investigation. This can include the observation of distinct vehicle traits and damage, partial license plates, bumper stickers, etc.

ALPRS data consists of license plate information and vehicle-related characteristics; it does not include personal identifying information about individuals. A license plate number is associated with a specific vehicle; additional investigative steps are required to identify any individual associated with that vehicle.

CCIC/NCIC Alerts

CCIC/NCIC alerts automatically update in the Axon ALPRS every six hours and in the state's mobile ELSAG ALPRS twice a day.

The approved alerts from NCIC/CCIC are the following:

- Gang or Suspected Terrorist
- Missing Person
- Stolen Plate
- Stolen Vehicle
- Warrants

Any recommended changes to the alerts that are visible to personnel in the Axon system will be submitted to the ALPRS Administrator. Any changes to this list require an update to this directive and approval through the department's policy review process before implementation.

Custom Hotlist Alerts

- Custom hotlist alerts in Axon can only be created by detectives, analysts, and patrol supervisors. Detectives and analysts must have supervisory approval to enter any custom hotlist alert. The supervisory approval will include the audience with whom the alert may be shared (e.g., entire department versus specific individuals).
- To be entered as a custom hotlist alert, the creator must ensure the following:
 - There is an active criminal investigation
 - There is reasonable suspicion that the vehicle included in the alert is a vehicle of a suspect in the crime or is a vehicle involved in the crime.
 - Essential details are included in the alert:
 - Creator's contact information;
 - Related case or incident number;
 - Brief synopsis for the reason for the alert; and
 - Clear actionable instructions (e.g., attempt to locate, detain if legal justification exists, no probable cause for arrest, for information only).
 - For detectives and analysts, the name of the supervisor that approved the alert.

- The alert does not include personal identifying information about individuals beyond what is necessary to identify the vehicle (e.g., license plate).
- Personnel are not allowed to create alerts accessible only to themselves. At a minimum, they must include their supervisor for oversight and auditing purposes.
- The creator of a custom hotlist alert is responsible for updating and removing entries as circumstances change (e.g., when a vehicle is recovered or no longer suspect).
- Custom hotlist alerts in Axon will automatically expire after 30 days.
- If an alert is still necessary after expiration, authorized personnel must enter a new alert following the steps in this written directive, including supervisory approval.

Case Reports

When an ALPRS is used to generate leads in an investigation that results in the identification of a suspect, vehicle, or other relevant details, and an arrest appears imminent, personnel will document the investigative process involving the use of the ALPRS to identify both inculpatory and exculpatory evidence. For example, if a vehicle is identified as a suspect in a robbery using the ALPRS, the personnel utilizing the system will document the methodology used to search for the vehicle and the specific steps taken to narrow the search to identify the vehicle. This documentation will include a summary of information obtained and general steps taken during the search process that led to the vehicle identification, which will be outlined in the case report or supplemental report. This process will ensure that the investigative steps taken are properly documented and available for discovery when the case is filed with the District Attorney's Office.

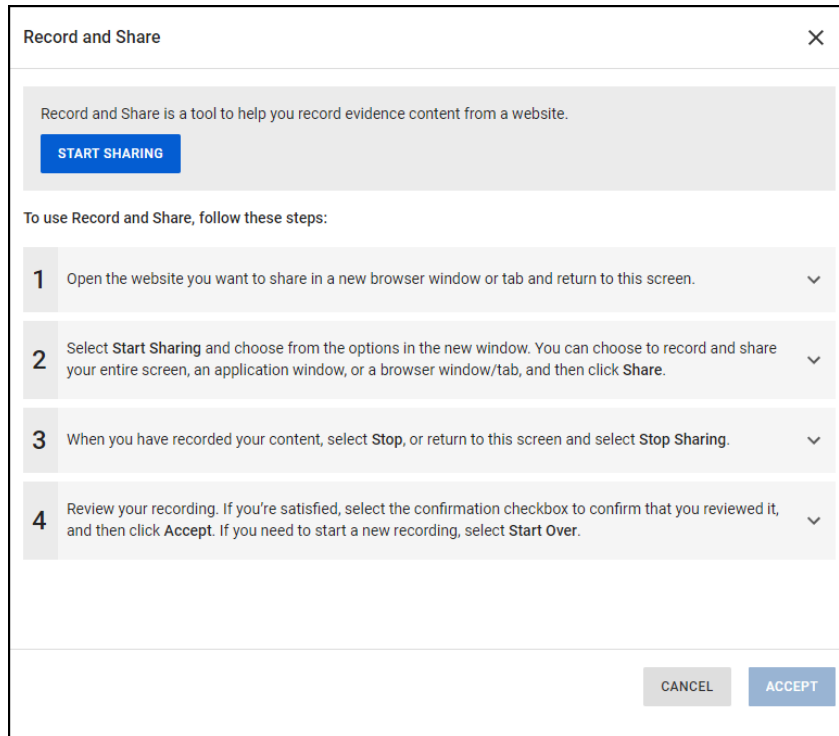
Officers and other personnel using ALPRS in their investigations will utilize Axon Evidence.com "Record and Share" to document the process and the steps taken to narrow the search parameters. This is a screen recording program that will directly import the actions taken visually into Evidence.com.

There are limitations to the "Record and Share" feature: The maximum file size is 4 Gigabytes, and the entire screen, window, or tab must be selected.

1. On the menu bar, click **Evidence** and then under the search filters, click **Import Evidence**.

The Import Evidence page appears.

2. To record website content, click **Record and Share**.
 - a. A panel will appear on the right side of the page. In the same browser, open a new window or tab and go to the website you want to record.



- b. Click **Start Sharing**, select the window or tab to record, and if audio should be recorded.
- c. When you are ready to stop recording, click **Stop** in the selected tab/window or **Stop Sharing** in the panel.
- d. You can add a Title, Evidence ID, and Category, as needed. Once you are ready to accept the recording, select the check box and click **Accept**.

Repeat this step to record other content.

3. Once the files are added, you can edit the Title, ID and Category information individually for each file. You can also edit the IDs and Categories for all the imported evidence or select and edit the IDs and Categories for specific files using the Edit All IDs and Edit All Categories options.

- a. Tag and Classify the video as appropriate with incident number and retention category.

If it is unknown at the time of capture if the search is going to be related to an incident that generates a case report, utilize the CAD Incident number and retention category: Non-Criminal Incident – All

Personnel will update the retention category once the incident becomes a case.

4. Click **Upload**

Reports will also contain specific information about how officers verified or corroborated that the vehicle identified was actually involved, including follow-up investigation(s) or evidence.

Documentation of Custom Hotlist Alerts

In addition, entries and actions related to custom hotlist alerts must be documented in case reports.

System Installation, Check Out, and Maintenance

Mobile ELSAG ALPRS

The Metro Division Motor Vehicle Theft Unit is responsible for overseeing the installation and maintenance of mobile ELSAG ALPRS.

Patrol officers will follow the proper procedures for checking out vehicles equipped with ELSAG ALPRS at their respective patrol divisions in the Quartermaster OnQ system.

Fixed and Mobile Axon ALPRS

The Management Services Division is responsible for overseeing the installation and maintenance of fixed and mobile Axon ALPRS.

Data Retention

ALPRS data collected by the department from Axon ALPRS is securely stored in a cloud-based system for a period of 30 days, after which the data is automatically purged unless it has been preserved as evidence in accordance with this directive.

ALPRS data collected by the department from mobile ELSAG ALPRS is stored in a state server with data retention schedules and purge procedures determined by the Colorado State Patrol (CSP). CSP set the retention period at 182 days.

When data has become evidence as part of an investigation, the applicable data will be downloaded from the server and placed into evidence by the investigating officer. When ALPRS data is identified as relevant to an investigation or potential evidentiary use, investigating officers will promptly preserve that data in accordance with department policy and Colorado law and will not rely on system retention periods for its availability.

Information Sharing

ALPRS data may only be shared for legitimate law enforcement and public safety purposes consistent with federal law, Colorado law, and department policy.

ALPRS data may be shared with other criminal justice agencies for official law enforcement purposes allowable under Colorado law. In accordance with [GO 305 Immigration and Foreign Nationals](#), department members shall not disclose this information for the purpose of identifying if the person has complied with civil or criminal federal immigration laws.

ALPRS data will not be shared for personal use or for any non-law enforcement purpose. Requests for ALPRS data from non-law enforcement entities, including private individuals, businesses, or the media, will be processed in accordance with the Colorado Criminal Justice Records Act (CCJRA) and department records release procedures.

The technology allows system-level information sharing with other law enforcement agencies. Employees are not permitted to use this feature. Only the ALPRS Administrator may make changes to the sharing settings, upon approval of the Deputy Chief of the Investigative and Special Operations Bureau via the chain of command.

Training

Personnel are not authorized to access the ALPRS until they have completed department training.

Personnel will receive ALPRS training from a designated trainer who attended a train-the-trainer course. The trainer is responsible for sending confirmation of completion to the attendee's lieutenant/manager and to the ALPRS Administrator. The lieutenant/manager will complete training registration in NeoGov.

Training must include the provisions of this written directive to ensure the proper and lawful use of the system. Training must include, but is not limited to, proper use of ALPRS, Colorado law, additional privacy considerations, and custom hotlist guidelines.

As part of training requirements, personnel will also read all written directives related to ALPRS and sign off on them in the department's online policy system before using any ALPR system.

Responsibilities of the ALPRS Administrator

- Maintain a roster of all approved ALPRS users for Axon and ELSAG
- Ensure training is available on NeoGov with training documentation automatically provided to the Training Division
- Grant access to authorized users and remove access as directed for both fixed and mobile ALPRS
- Complete records requests under Colorado Criminal Justice Records Act

- Conduct periodic audits of ALPRS data and system usage, and complete additional audits as requested, to ensure compliance with this directive.
- Ensure data retention period is set properly in databases controlled by the department